AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-27. (Canceled)

28. (Currently Amended) A computer emergency response system linked to a plurality of computer systems, the system comprising:

an information section configured to collect system information ~~for at least one of the plurality of computer systems~~ and security information related to ~~one or more~~ a security incident ~~incidents~~ that [[are]] is a threat to at least one of the plurality of computer systems;

a test bed configured to perform [[a]] an attack simulation ~~under a similar condition of~~ at the bed for the at least one computer system ~~of the plurality of computer systems~~ based on the system information and security information, under conditions similar to those of the at least one computer system; and

an assessment section configured to assess the ~~one or more~~ security incident ~~incidents~~ based on the simulation.

29. (Canceled)

30. (Currently Amended) The computer emergency response system of claim 28, wherein the assessment section assesses the ~~one or more~~ security incident ~~incidents~~ by classifying the ~~one or more~~ security incident ~~incidents~~ into one of several ~~or more~~ levels of attack.

31. (Currently Amended) The computer emergency response system of claim 30, further comprising an evaluation section configured to calculate expected damages ~~from an attack~~ based on the attack simulation and the assessed level of attack ~~at least one security incident with a similar level of attack~~.

32. (Currently Amended) The computer emergency response system of claim 31, further comprising an asset recovery section configured to provide an expected recovery time ~~from~~

~~the attack~~ for the at least one ~~of the plurality of~~ computer system ~~systems~~ based on the expected damages.

33. (Currently Amended) The computer emergency response system of claim 30, wherein the assessment section is further configured to provide a test ~~possible~~ scenario for [[an]] the attack simulation ~~on at least one of the plurality of computer systems~~ to the test bed, including a method of attack and frequency of attack.

34. (Currently Amended) The computer emergency response system of claim [[30]] 33, wherein the assessment section is further configured to ~~use the test bed to automatically assess the one or more security incidents~~ provide additional test scenarios for the attack simulation to the test bed until the security incident has been simulated on each of the plurality of computer systems.

35. (Currently Amended) The computer emergency response system of claim 30, wherein the assessment section is further ~~comprising an information sharing section~~ configured to classify the security information according to a method of attack, frequency of attack, and internet protocol address of a source of attack ~~and transfer the classified security information to at least one of the plurality of computer systems~~.

36. (Currently Amended) The computer emergency response system of claim 28, further comprising a warning section configured to issue an alert to the ~~simulated~~ at least one computer system based on [[an]] the assessment of the ~~one or more~~ security incident ~~incidents~~ by the assessment section, wherein the alert includes steps for responding to the security incident.

37. (Currently Amended) The computer emergency response system of claim 28, further comprising a warning section configured to issue a forecast to the ~~simulated~~ at least one computer system based on [[an]] the assessment of the ~~one or more~~ security incident[[s]] by the assessment section.

38. (Currently Amended) A method of simulating an attack in a computer emergency response system that is linked to a plurality of computer systems, the method comprising:

collecting system information ~~for at least one of the plurality of computer systems~~ and security information related to ~~one or more~~ a security incident ~~incidents~~ that [[are]] is a threat to at least one of the plurality of computer systems;

configuring a test bed to perform an attack simulation ~~under a similar condition of~~ at the test bed for the at least one computer system ~~of the plurality of computer systems~~based on the system information and security information, under conditions similar to those of the at least one computer system; and

performing an attack assessment for the ~~one or more~~ security incident ~~incidents~~ using the test bed.

39. (Canceled)

40. (Currently Amended) The method of claim 38, wherein the attack assessment classifies the ~~one or more~~ security incident ~~incidents~~ into one of several levels of attack.

41. (Currently Amended) The method of claim 40, further comprising calculating expected damage ~~to one or more of the plurality of computer systems from an attack~~ based on the attack simulation and assessed level of attack ~~at least one security incident with a similar level of attack~~.

42. (Currently Amended) The method of claim 41, further comprising calculating an expected recovery time ~~from the attack~~ for the at least one ~~of the plurality of~~ computer system ~~systems~~ based on the expected damage.

43. (Canceled)

44. (Currently Amended) The method of claim 38, further comprising providing a ~~possible~~ test scenario for [[an]] the attack simulation~~on at least one of the plurality of computer systems~~ to the test bed, including a method of attack and frequency of attack.

45. (Currently Amended) The method ~~computer emergency response system~~ of claim [[38]] 44, ~~wherein the performing of the attack assessment~~ further comprising providing additional test scenarios for the attack simulation to the test bed until the security incident has been simulated on each of the plurality of computer systems ~~is performed automatically for the one or more security incidents~~.

46. (Currently Amended) The method ~~computer emergency response system~~ of claim 38, further comprising classifying the security information according to a method of attack, time of attack, frequency of attack, internet protocol address of a source of the attack, internet service provider of the source of the attack, and country of origin of the source of the attack and ~~transferring~~ transmitting the classified security information and the attack assessment to ~~at least one of~~ the at least one ~~plurality of~~ computer system ~~systems~~.

47. (Currently Amended) The method ~~computer emergency response system~~ of claim 38, further comprising issuing an alert to the simulated computer system based on the attack assessment, wherein the alert includes steps for responding to the security incident in real time.

48. (Currently Amended) The method ~~computer emergency response system~~ of claim 38, further comprising issuing a forecast to the simulated computer system based on the attack assessment.

49. (Withdrawn) A computer readable medium having stored thereon computer executable components, the medium comprising:

an assessment section configured to provide an assessment which evaluates and classifies security information related to at least one security incident; and

a test bed section configured to simulate an attack on one or more other computing systems networked with a computing device based on the assessment and provide simulation results.

50. (Withdrawn) The computer readable medium of claim 49, further comprising a security section configured to protect the computing device from the one or more other computing systems based on the simulation results.

51. (Withdrawn) The computer readable medium of claim 49, wherein the attack simulation is further based on a database of security vulnerabilities of the one or more other computing systems.

52. (Withdrawn) The computer readable medium of claim 51, wherein the attack simulation determines whether the security vulnerabilities of the one or more other computing systems can be exploited based on the assessment.

53. (Withdrawn) The computer readable medium of claim 49, wherein the assessment is based on a frequency which the at least one security incident occurs.

54. (Withdrawn) The computer readable medium of claim 49, wherein the assessment is based on a comparison of the at least one security incident with other security incidents.

55. (Withdrawn) The computer readable medium of claim 49, further comprising a collection section configured to collect the security information from the one or more other computing systems.

56. (Withdrawn) The computer readable medium of claim 49, further comprising an information sharing section configured to send the assessment to at least one of the other computing systems.

57. (Withdrawn) The computer readable medium of claim 49, further comprising an information sharing section configured to send the simulation results to at least one of the other computing systems.

58. (Withdrawn) The computer readable medium of claim 49, wherein the at least one security incident relates to cyber terror.

59. (Withdrawn) A computer implemented method comprising:

determining an asset value for a computing device on a network; and

providing a damage calculation for a simulated attack on the computing device based on security information related to a security incident and the asset value.

60. (Withdrawn) The computer implemented method of claim 59, further comprising outputting the damage calculation to a display.

61. (Withdrawn) The computer implemented method of claim 59, wherein the security information comprises a likelihood of the security incident occurring.

62. (Withdrawn) The computer implemented method of claim 59, wherein the damage calculation is provided in monetary units.

63. (Withdrawn) The computer implemented method of claim 59, wherein the damage calculation provides an estimate of an amount of damage to the computing device from the simulated attack.

64. (Withdrawn) The computer implemented method of claim 59, wherein the security incident relates to a hacking.

65. (Withdrawn) The computer implemented method of claim 59, wherein the security incident relates to a worm.

66. (Withdrawn) The computer implemented method of claim 59, further comprising collecting the security information from one or more other computing systems on the network.

67. (Withdrawn) The computer implemented method of claim 59, further comprising:

determining a second asset value for a second computing device on the network; and

providing a second damage calculation for the simulated attack on the second computing device based on the security information and the second asset value.

68. (Withdrawn) The computer implemented method of claim 67, further comprising outputting the damage calculation and second damage calculation to a display.

69. (Withdrawn) A computer implemented comprising:

simulating an attack on a computing system based on a security vulnerability of the computing system and an exploit to the security vulnerability; and

generating a risk level for the computing system based on the simulation of the attack and an asset value of the computing system.

70. (Withdrawn) The computer implemented method of claim 69, wherein the security vulnerability comprises a service available on the computing system.

71. (Withdrawn) The computer implemented method of claim 69, wherein the security vulnerability comprises an application available on the computing system.

72. (Withdrawn) The computer implemented method of claim 69, wherein the asset value relates to the significance of the computing system.

73. (Withdrawn) The computer implemented method of claim 69, further comprising protecting the computing system based on the simulation of the attack.

74. (Withdrawn) The computer implemented method of claim 69, further comprising protecting a second computing system networked with the computing system based on the simulation of the attack.

75. (New) The computer emergency response system of claim 35, further comprising an information sharing section configured to transmit the classified security information and the attack assessment to the at least one computer system.

76. (New) The computer emergency response system of claim 31, wherein the evaluation section is further configured to calculate the expected damages in categories of network exposure, system exposure, system service delay, and network service delay.

77. (New) The computer emergency response system of claim 76, wherein the evaluation section is further configured to calculate the expected damages in categories of root authority acquisition, data release, and data forgery.

78. (New) The computer emergency response system of claim 76, further comprising an information sharing section configured to transmit the expected damages to the at least one computer system.

79. (New) The computer emergency response system of claim 33, further comprising:

a training section configured to generate training data based on the attack simulation, the training data configured to train the at least one computer system to prevent the security incident; and

an information sharing section configured to transmit the training data to the at least one computer system.

80. (New) The computer emergency response system of claim 28, further comprising a warning section configured to issue an alert to the at least one computer system based on the assessment of the security incident by the assessment section, wherein the alert includes steps for preventing the security incident.